National Critical Information Infrastructure Protection Centre

CVE Report

16-30 June 2017 **Vol. 04 No. 10**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Acronis					
True Image					
NA	21-06-2017	8.3	Acronis True Image up to and including version 2017 Build 8053 performs software updates using HTTP. Downloaded updates are only verified using a server-provided MD5 hash. **CVE ID: CVE-2017-3219**	NA	A-ACR-TRUE -050717/01
Adobe					
Captivate					
Gain Information	20-06-2017	5	Adobe Captivate versions 9 and earlier have an information disclosure vulnerability resulting from abuse of the quiz reporting feature in Captivate. **CVE ID: CVE-2017-3087**	https://helpx.adobe.com/security/products/captivate/apsb17-19.html	A-ADO-CAPTI-050717/02
Execute Code	20-06-2017	10	Adobe Captivate versions 9 and earlier have a remote code execution vulnerability in the quiz reporting feature that could be abused to read and write arbitrary files to the server. **CVE ID: CVE-2017-3098**	https://helpx.adobe.com/security/products/captivate/apsb17-19.html	A-ADO-CAPTI-050717/03
Digital Editions					
Execute Code	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading functions in the installer plugin. A successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3097**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/04
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the character code mapping module. Successful exploitation could lead to	https://helpx.adobe.com/security/products/Digital-	A-ADO-DIGIT-050717/05

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			arbitrary code execution. **CVE ID: CVE-2017-3096**	Editions/apsb17-20.html	
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF parsing engine. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3095**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/06
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF processing engine. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3094**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/07
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the bitmap representation module. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3093**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/08
Execute Code	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading of editor control library functions in the installer plugin. A successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3092**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/09
Execute Code	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier contain an insecure library loading vulnerability. The vulnerability is due to unsafe library loading of browser related library extensions in the installer plugin. A successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/10

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-3090		
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF imaging model. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3089**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/11
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Digital Editions versions 4.5.4 and earlier have an exploitable memory corruption vulnerability in the PDF runtime engine. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3088**	https://helpx.adobe.com/security/products/Digital-Editions/apsb17-20.html	A-ADO-DIGIT-050717/12
Flash Player					
Execute Code	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the advertising metadata functionality. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3084**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/13
Execute Code	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the Primetime SDK functionality related to the profile metadata of the media stream. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3083**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/14
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the LocaleID class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3082**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/15
Execute Code	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability during internal computation caused by	https://helpx.adobe.com/security/products/flash	A-ADO-FLASH-050717/16

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			multiple display object mask manipulations. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3081**	-player/apsb17-17.html	
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the internal representation of raster data. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3079**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/17
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the Adobe Texture Format (ATF) module. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3078**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/18
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the PNG image parser. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3077**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/19
Execute Code Overflow Memory Corruption	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the MPEG-4 AVC module. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3076**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/20
Execute Code	20-06-2017	10	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability when manipulating the ActionsScript 2 XML class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3075**	https://helpx.adobe.com/security/products/flash-player/apsb17-17.html	A-ADO-FLASH-050717/21
Shockwave Player					
Execute Code Overflow	20-06-2017	10	Adobe Shockwave versions 12.2.8.198 and earlier have an exploitable	https://helpx.adobe.com	A-ADO-SHOCK-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Memory Corruption		🟥	memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3086**	/security/products/shockwave/apsb17-18.html	050717/22
Apache					
Httpd					
Overflow	19-06-2017	7.5	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header. **CVE ID: CVE-2017-7679**	NA	A-APA-HTTPD-050717/23
NA	19-06-2017	7.5	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value. **CVE ID: CVE-2017-7668**	NA	A-APA-HTTPD-050717/24
NA	19-06-2017	7.5	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. **CVE ID: CVE-2017-3169**	NA	A-APA-HTTPD-050717/25
Bypass	19-06-2017	7.5	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. **CVE ID: CVE-2017-3167**	NA	A-APA-HTTPD-050717/26
Thrift					
DoS	16-06-2017	4	The client libraries in Apache Thrift before 0.9.3 might allow remote authenticated users to cause a denial of service (infinite recursion) via vectors involving the skip function. **CVE ID: CVE-2015-3254**	https://issues.apache.org/jira/browse/THRIFT-3231	A-APA-THRIF-050717/27

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Audiocoding					
Freeware Advanced Audio Coder					
DoS	21-06-2017	4.3	The faacEncOpen function in libfaac/frame.c in Freeware Advanced Audio Coder (FAAC) 1.28 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file. **CVE ID: CVE-2017-9130**	https://www.exploit-db.com/exploits/42207/	A-AUD-FREEW-050717/28
Freeware Advanced Audio Decoder 2					
DoS	27-06-2017	4.3	The mp4ff_read_stts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9223**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/29
DoS	27-06-2017	4.3	The mp4ff_read_mdhd function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9221**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/30
DoS Overflow	27-06-2017	4.3	The mp4ff_read_stco function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (memory allocation error) via a crafted mp4 file. **CVE ID: CVE-2017-9220**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/31
DoS Overflow	27-06-2017	4.3	The mp4ff_read_stsc function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (memory allocation error and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9219**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/32
DoS	27-06-2017	4.3	The mp4ff_read_stsd function in common/mp4ff/mp4atom.c in	http://seclists.org/fulldi	A-AUD-FREEW-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9218**	sclosure/2017/Jun/32	050717/33
DoS	27-06-2017	7.1	The mp4ff_read_ctts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9257**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/34
DoS	27-06-2017	7.1	The mp4ff_read_stco function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9256**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/35
DoS	27-06-2017	7.1	The mp4ff_read_stsc function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9255**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/36
DoS	27-06-2017	7.1	The mp4ff_read_stts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9254**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/37
DoS	27-06-2017	7.1	The mp4ff_read_stsd function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/38

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			mp4 file. **CVE ID: CVE-2017-9253**		
DoS	27-06-2017	7.1	The mp4ff_parse_tag function in common/mp4ff/mp4meta.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9222**	http://seclists.org/fulldisclosure/2017/Jun/32	A-AUD-FREEW-050717/39
BOA					
BOA					
Directory Traversal	23-06-2017	5	/cgi-bin/wapopen in BOA Webserver 0.94.14rc21 allows the injection of "../.." using the FILECAMERA variable (sent by GET) to read files with root privileges. **CVE ID: CVE-2017-9833**	https://pastebin.com/raw/rt7LJvyF	A-BOA-BOA-050717/40
Bradynationalbank					
Bnb Mobile Banking					
Gain Information	16-06-2017	4.3	The "BNB Mobile Banking" by Brady National Bank app 3.0.0 -- aka bnb-mobile-banking/id674215747 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9582**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-BRA-BNB M-050717/41
Cagintranetworks					
Getsimple Cms					
XSS	29-06-2017	4.3	admin/profile.php in GetSimple CMS 3.x has XSS in a name field. **CVE ID: CVE-2017-10673**	https://github.com/GetSimpleCMS/GetSimpleCMS/issues/1234	A-CAG-GETSI-050717/42
Cayugalakenationalbank					
Cayuga Lake National Bank					
Gain	16-06-2017	4.3	The cayuga-lake-national-	https://med	A-CAY-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Information			bank/id1151601539 app 4.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9560**	ium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	CAYUG-050717/43
Check Mk Project					
Check Mk					
XSS	21-06-2017	4.3	A cross site scripting (XSS) vulnerability exists in Check_MK versions 1.4.0x prior to 1.4.0p6, allowing an unauthenticated remote attacker to inject arbitrary HTML or JavaScript via the _username parameter when attempting authentication to webapi.py, which is returned unencoded with content type text/html. **CVE ID: CVE-2017-9781**	http://git.mathias-kettner.de/git/?p=check_mk.git;a=blob;f=.werks/4757;hb=c248f0b6ff7b15ced9f07a3df8a80fad656ea5b1	A-CHE-CHECK-050717/44
Cisco					
Evolved Programmable Network Manager; Prime Infrastructure					
Execute Code	26-06-2017	6	A vulnerability in the web-based user interface of Cisco Prime Infrastructure (PI) and Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker read and write access to information stored in the affected system as well as perform remote code execution. The attacker must have valid user credentials. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing an XML file. An attacker could exploit this vulnerability by convincing the administrator of an affected system to import a crafted XML file with malicious entries which could allow the attacker to read and write files and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm1	A-CIS-EVOLV-050717/45

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			execute remote code within the application, aka XML Injection. Cisco Prime Infrastructure software releases 1.1 through 3.1.6 are vulnerable. Cisco EPNM software releases 1.2, 2.0, and 2.1 are vulnerable. Cisco Bug IDs: CSCvc23894 CSCvc49561. **CVE ID: CVE-2017-6662**		
Virtualized Packet Core					
DoS	26-06-2017	7.8	A vulnerability in the ingress UDP packet processing functionality of Cisco Virtualized Packet Core-Distributed Instance (VPC-DI) Software 19.2 through 21.0 could allow an unauthenticated, remote attacker to cause both control function (CF) instances on an affected system to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient handling of user-supplied data by the affected software. An attacker could exploit this vulnerability by sending crafted UDP packets to the distributed instance (DI) network addresses of both CF instances on an affected system. A successful exploit could allow the attacker to cause an unhandled error condition on the affected system, which would cause the CF instances to reload and consequently cause the entire VPC to reload, resulting in the disconnection of all subscribers and a DoS condition on the affected system. This vulnerability can be exploited via IPv4 traffic only. Cisco Bug IDs: CSCvc01665 CSCvc35565. **CVE ID: CVE-2017-6678**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-vpc	A-CIS-VIRTU-050717/46
Webex Arf Player					
Execute Code Overflow	26-06-2017	6.8	Multiple buffer overflow vulnerabilities exist in the Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) files. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurit	A-CIS-WEBEX-050717/47

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			vulnerabilities by providing a user with a malicious ARF file via email or URL and convincing the user to launch the file. Exploitation of these vulnerabilities could cause an affected player to crash and, in some cases, could allow arbitrary code execution on the system of a targeted user. The Cisco WebEx Network Recording Player is an application that is used to play back WebEx meeting recordings that have been recorded on the computer of an online meeting attendee. The player can be automatically installed when the user accesses a recording file that is hosted on a WebEx server. The following client builds are affected by this vulnerability: Cisco WebEx Business Suite (WBS29) client builds prior to T29.13.130, Cisco WebEx Business Suite (WBS30) client builds prior to T30.17, Cisco WebEx Business Suite (WBS31) client builds prior to T31.10. Cisco Bug IDs: CSCvc47758 CSCvc51227 CSCvc51242. **CVE ID: CVE-2017-6669**	yAdvisory/cisco-sa-20170621-wnrp	
Cmsmadesimple					
Cms Made Simple					
XSS	18-06-2017	4.3	In admin\addgroup.php in CMS Made Simple 2.1.6, when adding a user group, there is no XSS filtering, resulting in storage-type XSS generation, via the description parameter in an addgroup action. **CVE ID: CVE-2017-9668**	https://github.com/XiaoZhis/ProjectSend/issues/2	A-CMS-CMS M-050717/48
Cognito					
Moneyworks					
NA	26-06-2017	5	Password exposure in Cognito Software Moneyworks 8.0.3 and earlier allows attackers to gain administrator access to all data, because verbose logging writes the administrator password to a world-		A-COG-MONEY-050717/49

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			readable file. **CVE ID: CVE-2017-9615**		
Dolibarr					
Dolibarr					
Execute Code	25-06-2017	6.5	Dolibarr ERP/CRM 5.0.3 and prior allows low-privilege users to upload files of dangerous types, which can result in arbitrary code execution within the context of the vulnerable application. **CVE ID: CVE-2017-9840**	https://www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-009	A-DOL-DOLIB-050717/50
Easysitecms					
Easysite					
Execute Code Sql	24-06-2017	7.5	SQL injection vulnerability in C_InfoService.asmx in WebServices in Easysite 7.0 could allow remote attackers to execute arbitrary SQL commands via an XML document containing a crafted ArticleIDs element within a GetArticleHitsArray element. **CVE ID: CVE-2017-9848**	http://www.2cto.com/article/201409/338712.html	A-EAS-EASYS-050717/51
Ecava					
Integraxor					
Execute Code Sql	21-06-2017	7.5	A SQL Injection issue was discovered in Ecava IntegraXor Versions 5.2.1231.0 and prior. The application fails to properly validate user input, which may allow for an unauthenticated attacker to remotely execute arbitrary code in the form of SQL queries. **CVE ID: CVE-2017-6050**		A-ECA-INTEG-050717/52
Elasticsearch					
Kibana					
XSS	16-06-2017	4.3	Kibana before 4.5.4 and 4.1.11 are vulnerable to an XSS attack that would allow an attacker to execute arbitrary JavaScript in users' browsers. **CVE ID: CVE-2016-1000220**	https://www.elastic.co/community/security	A-ELA-KIBAN-050717/53
XSS	16-06-2017	4.3	Kibana versions after and including 4.3 and before 4.6.2 are vulnerable to a cross-site scripting (XSS) attack.	https://www.elastic.co/community/	A-ELA-KIBAN-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2016-10366	security	54
XSS	16-06-2017	4.3	Kibana versions prior to 4.1.3 and 4.2.1 are vulnerable to a XSS attack. **CVE ID: CVE-2015-9056**	https://www.elastic.co/community/security	A-ELA-KIBAN-050717/55
NA	16-06-2017	5	Kibana versions prior to 5.2.1 configured for SSL client access, file descriptors will fail to be cleaned up after certain requests and will accumulate over time until the process crashes. **CVE ID: CVE-2017-8452**	https://www.elastic.co/community/security	A-ELA-KIBAN-050717/56
NA	16-06-2017	5	Kibana before 4.5.4 and 4.1.11 when a custom output is configured for logging in, cookies and authorization headers could be written to the log files. This information could be used to hijack sessions of other users when using Kibana behind some form of authentication such as Shield. **CVE ID: CVE-2016-1000219**	https://www.elastic.co/community/security	A-ELA-KIBAN-050717/57
NA	16-06-2017	5.8	Kibana versions before 4.6.3 and 5.0.1 have an open redirect vulnerability that would enable an attacker to craft a link in the Kibana domain that redirects to an arbitrary website. **CVE ID: CVE-2016-10365**	https://www.elastic.co/community/security	A-ELA-KIBAN-050717/58
Logstash					
NA	16-06-2017	5	Logstash prior to version 2.1.2, the CSV output can be attacked via engineered input that will create malicious formulas in the CSV data. **CVE ID: CVE-2016-1000222**	https://www.elastic.co/community/security	A-ELA-LOGST-050717/59
Gain Information	16-06-2017	5	Logstash prior to version 2.3.4, Elasticsearch Output plugin would log to file HTTP authorization headers which could contain sensitive information. **CVE ID: CVE-2016-1000221**	https://www.elastic.co/community/security	A-ELA-LOGST-050717/60
Fedoraproject					
Arm Installer					
NA	26-06-2017	4.4	fedora-arm-installer up to and including 1.99.16 is vulnerable to local privilege escalation due to lack of	https://pagure.io/arm-image-	A-FED-ARM I-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			checking the error condition of mount operation failure on unsafely created temporary directories. **CVE ID: CVE-2017-7496**	installer/pull-request/10	61
Ffmpeg					
Ffmpeg					
DoS Overflow	28-06-2017	6.8	libavcodec/scpr.c in FFmpeg 3.3 before 3.3.1 does not properly validate height and width data, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **CVE ID: CVE-2017-9995**	NA	A-FFM-FFMPE-050717/62
Flatpak					
Flatpak					
NA	21-06-2017	7.2	In Flatpak before 0.8.7, a third-party app repository could include malicious apps that contain files with inappropriate permissions, for example setuid or world-writable. The files are deployed with those permissions, which would let a local attacker run the setuid executable or write to the world-writable location. In the case of the "system helper" component, files deployed as part of the app are owned by root, so in the worst case they could be setuid root. **CVE ID: CVE-2017-9780**	https://github.com/flatpak/flatpak/issues/845	A-FLA-FLATP-050717/63
Fountaintrust					
Fountain Trust Mobile Banking					
Gain Information	16-06-2017	4.3	The "Fountain Trust Mobile Banking" by FOUNTAIN TRUST COMPANY app 3.0.0 -- aka fountain-trust-mobile-banking/id891343006 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9599**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85	A-FOU-FOUNT-050717/64

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

				c5	
Freedesktop					
Poppler					
DoS Overflow	22-06-2017	4.3	Stack buffer overflow in GfxState.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) via a crafted PDF document. **CVE ID: CVE-2017-9775**	https://bugs.freedesktop.org/show_bug.cgi?id=101540	A-FRE-POPPL-050717/65
DoS Overflow	25-06-2017	4.3	The function GfxImageColorMap::getGray in GfxState.cc in Poppler 0.54.0 allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted PDF document, related to missing color-map validation in ImageOutputDev.cc. **CVE ID: CVE-2017-9865**		A-FRE-POPPL-050717/66
DoS Overflow	22-06-2017	6.8	Integer overflow leading to Heap buffer overflow in JBIG2Stream.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document. **CVE ID: CVE-2017-9776**	https://bugs.freedesktop.org/show_bug.cgi?id=101541	A-FRE-POPPL-050717/67
Fsbbigfork					
First State Bank Of Bigfork Mobile Banking					
Gain Information	16-06-2017	4.3	The "First State Bank of Bigfork Mobile Banking" by First State Bank of Bigfork app 4.0.3 -- aka first-state-bank-of-bigfork-mobile-banking/id1133969876 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9595**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-FSB-FIRST-050717/68
Glpi-project					
Glpi					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Execute Code Sql	21-06-2017	6	Multiple SQL injection vulnerabilities in GLPI 0.90.4 allow an authenticated remote attacker to execute arbitrary SQL commands by using a certain character when the database is configured to use Big5 Asian encoding. **CVE ID: CVE-2016-7508**	https://github.com/glpi-project/glpi/issues/1047	A-GLP-GLPI-050717/69
GNU					
Binutils					
DoS Overflow	26-06-2017	4.3	The get_build_id function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file in which a certain size field is larger than a corresponding data field, as demonstrated by mishandling within the objdump program. **CVE ID: CVE-2017-9955**	https://sourceware.org/bugzilla/show_bug.cgi?id=21665	A-GNU-BINUT-050717/70
DoS Overflow	26-06-2017	4.3	The getvalue function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted tekhex file, as demonstrated by mishandling within the nm program. **CVE ID: CVE-2017-9954**		A-GNU-BINUT-050717/71
DoS Execute Code Overflow	19-06-2017	6.8	The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9756**	https://sourceware.org/bugzilla/show_bug.cgi?id=21595	A-GNU-BINUT-050717/72
DoS Execute Code Overflow	19-06-2017	6.8	opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows	https://sourceware.org/bugzilla/sho	A-GNU-BINUT-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9755**	w_bug.cgi?id=21594	73
DoS Overflow	19-06-2017	6.8	The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not validate a certain offset, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9754**	https://sourceware.org/bugzilla/show_bug.cgi?id=21591	A-GNU-BINUT-050717/74
DoS Overflow	19-06-2017	6.8	The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not initialize a certain data structure, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9753**	https://sourceware.org/bugzilla/show_bug.cgi?id=21591	A-GNU-BINUT-050717/75
DoS Overflow	19-06-2017	6.8	bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file in the	https://sourceware.org/bugzilla/show_bug.cgi?id=21589	A-GNU-BINUT-050717/76

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			_bfd_vms_get_value and _bfd_vms_slurp_etir functions during "objdump -D" execution. **CVE ID: CVE-2017-9752**		
DoS Execute Code Overflow	19-06-2017	6.8	opcodes/rl78-decode.opc in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9751**	https://sourceware.org/bugzilla/show_bug.cgi?id=21588	A-GNU-BINUT-050717/77
DoS Execute Code Overflow	19-06-2017	6.8	opcodes/rx-decode.opc in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9750**	https://sourceware.org/bugzilla/show_bug.cgi?id=21587	A-GNU-BINUT-050717/78
DoS Execute Code Overflow	19-06-2017	6.8	The *regs* macros in opcodes/bfin-dis.c in GNU Binutils 2.28 allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9749**	https://sourceware.org/bugzilla/show_bug.cgi?id=21586	A-GNU-BINUT-050717/79
DoS Overflow	19-06-2017	6.8	The ieee_object_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted	https://sourceware.org/bugzilla/show_bug.cgi?id=21582	A-GNU-BINUT-050717/80

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug. **CVE ID: CVE-2017-9748**		
DoS Overflow	19-06-2017	6.8	The ieee_archive_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. NOTE: this may be related to a compiler bug. **CVE ID: CVE-2017-9747**	https://sourceware.org/bugzilla/show_bug.cgi?id=21581	A-GNU-BINUT-050717/81
DoS Overflow	19-06-2017	6.8	The disassemble_bytes function in objdump.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns printing for this file during "objdump -D" execution. **CVE ID: CVE-2017-9746**	https://sourceware.org/bugzilla/show_bug.cgi?id=21580	A-GNU-BINUT-050717/82
DoS Overflow	19-06-2017	6.8	The _bfd_vms_slurp_etir function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9745**	https://sourceware.org/bugzilla/show_bug.cgi?id=21579	A-GNU-BINUT-050717/83
DoS Overflow	19-06-2017	6.8	The sh_elf_set_mach_from_flags function in bfd/elf32-sh.c in the Binary File Descriptor (BFD) library (aka	https://sourceware.org/bugzilla/sho	A-GNU-BINUT-050717/

			libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9744**	w_bug.cgi?id=21578	84
DoS Execute Code Overflow	19-06-2017	6.8	The print_insn_score32 function in opcodes/score7-dis.c:552 in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9743**	NA	A-GNU-BINUT-050717/85
DoS Execute Code Overflow	19-06-2017	6.8	The score_opcodes function in opcodes/score7-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during "objdump -D" execution. **CVE ID: CVE-2017-9742**	https://sourceware.org/bugzilla/show_bug.cgi?id=21576	A-GNU-BINUT-050717/86
GDB					
NA	21-06-2017	4.3	GNU Debugger (GDB) 8.0 and earlier fails to detect a negative length field in a DWARF section. A malformed section in an ELF binary or a core file can cause GDB to repeatedly allocate memory until a process limit is reached. This can, for example, impede efforts to analyze malware with GDB. **CVE ID: CVE-2017-9778**	https://sourceware.org/bugzilla/show_bug.cgi?id=21600	A-GNU-GDB-050717/87
Gnutls					
NA	16-06-2017	5	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid	https://www.gnutls.org/security.html#GNUTLS	A-GNU-GNUTL-050717/88

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			contents. This could lead to a crash of the GnuTLS server application. **CVE ID: CVE-2017-7507**	-SA-2017-4	
Ncurses					
Execute Code	29-06-2017	7.5	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack. **CVE ID: CVE-2017-10685**	https://bugzilla.redhat.com/show_bug.cgi?id=1464692	A-GNU-NCURS-050717/89
Execute Code Overflow	29-06-2017	7.5	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack. **CVE ID: CVE-2017-10684**	https://bugzilla.redhat.com/show_bug.cgi?id=1464687	A-GNU-NCURS-050717/90
Horde					
Horde Image Api					
Execute Code	21-06-2017	6.5	Remote Code Execution was found in Horde_Image 2.x before 2.5.0 via a crafted GET request. Exploitation requires authentication. **CVE ID: CVE-2017-9774**	https://lists.horde.org/archives/announce/2017/001234.html	A-HOR-HORDE-050717/91
IBM					
Curam Social Program Management					
XSS	28-06-2017	3.5	IBM Curam Social Program Management 5.2, 6.0, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 120744. **CVE ID: CVE-2017-1106**	http://www.ibm.com/support/docview.wss?uid=swg22004580	A-IBM-CURAM-050717/92
Data Server Client; Data Server Driver For Odbc And Cli; Data Server Driver Package; Data Server Runtime Client; DB2; Db2 Connect					
DoS Overflow	27-06-2017	3.6	IBM DB2 for Linux, UNIX and Windows 9.2, 10.1, 10.5, and 11.1 (includes DB2 Connect Server) is vulnerable to a buffer overflow that could allow a local user to overwrite DB2 files or cause a denial of service. IBM X-Force ID: 120668.	http://www.ibm.com/support/docview.wss?uid=swg22003877	A-IBM-DATA -050717/93

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-1105		
Execute Code Overflow	27-06-2017	4.4	IBM DB2 for Linux, UNIX and Windows 9.2, 10.1, 10.5, and 11.1 (includes DB2 Connect Server) is vulnerable to a stack-based buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code. IBM X-Force ID: 125159. **CVE ID: CVE-2017-1297**	http://www.ibm.com/support/docview.wss?uid=swg22004878	A-IBM-DATA -050717/94
Informix Dynamic Server					
Overflow	29-06-2017	4	IBM Informix Dynamic Server 12.1 could allow an authenticated user to cause a buffer overflow that would write large assertion fail files to the server. Done enough times, this could use large parts of the file system and cause the server to crash. IBM X-Force ID: 125569. **CVE ID: CVE-2017-1310**	http://www.ibm.com/support/docview.wss?uid=swg22004930	A-IBM-INFOR-050717/95
Qradar Security Information And Event Manager					
XSS	27-06-2017	3.5	IBM QRadar 7.2 and 7.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 123913. **CVE ID: CVE-2017-1234**	http://www.ibm.com/support/docview.wss?uid=swg22004948	A-IBM-QRADA-050717/96
Gain Information	27-06-2017	4.3	IBM QRadar 7.2 and 7.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 120208. **CVE ID: CVE-2016-9972**	http://www.ibm.com/support/docview.wss?uid=swg22004925	A-IBM-QRADA-050717/97
NA	27-06-2017	5	IBM QRadar 7.2 and 7.3 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID:	http://www.ibm.com/support/docview.wss?uid=swg220049	A-IBM-QRADA-050717/98

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			119783. **CVE ID: CVE-2016-9738**	26	
Rational Collaborative Lifecycle Management;Rational Engineering Lifecycle Manager					
XSS	22-06-2017	3.5	IBM RELM 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID: CVE-2016-9747**	http://www.ibm.com/support/docview.wss?uid=swg22004734	A-IBM-RATIO-050717/99
Sterling B2b Integrator					
Gain Information	23-06-2017	2.1	IBM Sterling B2B Integrator Standard Edition 5.2 stores potentially sensitive information from HTTP sessions that could be read by a local user. IBM X-Force ID: 126525. **CVE ID: CVE-2017-1349**	http://www.ibm.com/support/docview.wss?uid=swg22004209	A-IBM-STERL-050717/100
Gain Information	23-06-2017	2.1	IBM Sterling B2B Integrator Standard Edition 5.2 could allow a local user view sensitive information due to improper access controls. IBM X-Force ID: 125456. **CVE ID: CVE-2017-1302**	http://www.ibm.com/support/docview.wss?uid=swg22004202	A-IBM-STERL-050717/101
Gain Information	23-06-2017	2.1	IBM Sterling B2B Integrator Standard Edition 5.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 115336. **CVE ID: CVE-2016-5893**	http://www.ibm.com/support/docview.wss?uid=swg22004272	A-IBM-STERL-050717/102
Gain Information	22-06-2017	3.5	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user with special privileges to view files that they should not have access to. IBM X-Force ID: 120275. **CVE ID: CVE-2016-9983**	http://www.ibm.com/support/docview.wss?uid=swg22004273	A-IBM-STERL-050717/103
XSS	23-06-2017	3.5	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure	http://www.ibm.com/support/docview.wss?uid=swg22004199	A-IBM-STERL-050717/104

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			within a trusted session. IBM X-Force ID: 126524. **CVE ID: CVE-2017-1348**		
XSS	23-06-2017	3.5	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 121418. **CVE ID: CVE-2017-1132**	http://www.ibm.com/support/docview.wss?uid=swg22004199	A-IBM-STERL-050717/105
	22-06-2017	4	IBM Sterling File Gateway does not properly restrict user requests based on permission level. This allows for users to update data related to other users, by manipulating the parameters passed in the POST request. IBM X-Force ID: 126060. **CVE ID: CVE-2017-1326**	http://www.ibm.com/support/docview.wss?uid=swg22004274	A-IBM-STERL-050717/106
Gain Information	22-06-2017	4	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user to obtain sensitive information such as account lists due to improper access control. IBM X-Force ID: 120274. **CVE ID: CVE-2016-9982**	http://www.ibm.com/support/docview.wss?uid=swg22004273	A-IBM-STERL-050717/107
Gain Information	23-06-2017	4	IBM Sterling B2B Integrator Standard Edition 5.2 could allow user to obtain sensitive information using an HTTP GET request. IBM X-Force ID: 123667. **CVE ID: CVE-2017-1193**	http://www.ibm.com/support/docview.wss?uid=swg22004202	A-IBM-STERL-050717/108
Gain Information	23-06-2017	4	IBM Sterling B2B Integrator Standard Edition 5.2 could allow an authenticated user to obtain sensitive information by using unsupported, specially crafted HTTP commands. IBM X-Force ID: 121375. **CVE ID: CVE-2017-1131**	http://www.ibm.com/support/docview.wss?uid=swg22004270	A-IBM-STERL-050717/109
Sql	23-06-2017	6.5	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to SQL injection. A remote attacker could send	http://www.ibm.com/support/docvi	A-IBM-STERL-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 126462. **CVE ID: CVE-2017-1347**	ew.wss?uid=swg22004199	110
Websphere Mq					
DoS	21-06-2017	3.5	IBM WebSphere MQ 8.0 and 9.0 could allow an authenticated user to cause a denial of service to the MQXR channel when trace is enabled. IBM X-Force ID: 121155. **CVE ID: CVE-2017-1117**	http://www.ibm.com/support/docview.wss?uid=swg22001468	A-IBM-WEBSP-050717/111
Ideablade					
Breeze.server.net					
Execute Code	22-06-2017	7.5	IdeaBlade Breeze Breeze.Server.NET before 1.6.5 allows remote attackers to execute arbitrary code, related to use of TypeNameHandling in JSON deserialization. **CVE ID: CVE-2017-9424**	NA	A-IDE-BREEZ-050717/112
Ipfire					
Ipfire					
CSRF	19-06-2017	6.5	IPFire 2.19 has a Remote Command Injection vulnerability in ids.cgi via the OINKCODE parameter, which is mishandled by a shell. This can be exploited directly by authenticated users, or through CSRF. **CVE ID: CVE-2017-9757**	NA	A-IPF-IPFIR-050717/113
Irfanview					
Irfanview					
Execute Code Overflow	21-06-2017	6.8	An exploitable integer overflow vulnerability exists in the JPEG 2000 parser functionality of IrfanView 4.44. A specially crafted jpeg2000 image can cause an integer overflow leading to wrong memory allocation resulting in arbitrary code execution. Vulnerability can be triggered by viewing the image in via the application or by using thumbnailing feature of IrfanView. **CVE ID: CVE-2017-2813**	NA	A-IRF-IRFAN-050717/114

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Jasper Project					
Jasper					
DoS Overflow	21-06-2017	4.3	JasPer 2.0.12 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted image, related to the jp2_decode function in libjasper/jp2/jp2_dec.c. **CVE ID: CVE-2017-9782**	https://github.com/mdadams/jasper/issues/140	A-JAS-JASPE-050717/115
Lame Project					
Lame					
DoS Overflow	25-06-2017	4.3	The III_i_stereo function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file. **CVE ID: CVE-2017-9870**	NA	A-LAM-LAME-050717/116
DoS Overflow	25-06-2017	4.3	The II_step_one function in layer2.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file. **CVE ID: CVE-2017-9869**	NA	A-LAM-LAME-050717/117
DoS Overflow	25-06-2017	4.3	The fill_buffer_resample function in util.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file. **CVE ID: CVE-2015-9101**	NA	A-LAM-LAME-050717/118
DoS	25-06-2017	4.3	The fill_buffer_resample function in util.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted audio file. **CVE ID: CVE-2015-9100**	NA	A-LAM-LAME-050717/119
DoS	25-06-2017	4.3	The lame_init_params function in lame.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a	NA	A-LAM-LAME-050717/

			denial of service (invalid read and application crash) via a crafted audio file with a negative sample rate. **CVE ID: CVE-2015-9099**		120
DoS Overflow	25-06-2017	6.8	The III_dequantize_sample function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file. **CVE ID: CVE-2017-9872**	NA	A-LAM-LAME-050717/121
DoS Overflow	25-06-2017	6.8	The III_i_stereo function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file. **CVE ID: CVE-2017-9871**	NA	A-LAM-LAME-050717/122
Lbtc					
Lee Bank & Trust					
Gain Information	16-06-2017	4.3	The Lee Bank & Trust lbtc-mobile/id1068984753 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9561**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-LBT-LEE B-050717/123
Lenovo					
Advanced Settings Utility; Toolscenter Dynamic System Analysis; Updatexpress System Pack Installer					
Gain Information	19-06-2017	3.5	If multiple users are concurrently logged into a single system where one user is sending a command via the Lenovo ToolsCenter Advanced Settings	https://support.lenovo.com/us/en/product_sec	A-LEN-ADVAN-050717/124

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Utility (ASU), UpdateXpress System Pack Installer (UXSPI) or Dynamic System Analysis (DSA) to a second machine, the other users may be able to see the user ID and clear text password that were used to access the second machine during the time the command is processing. **CVE ID: CVE-2017-3743**	urity/LEN-10810	
Xclarity Administrator					
Gain Privileges	19-06-2017	2.1	In Lenovo XClarity Administrator (LXCA) before 1.3.0, if service data is downloaded from LXCA, a non-administrative user may have access to password information for users that have previously authenticated to the LXCA's internal LDAP server, including administrative accounts and service accounts with administrative privileges. This is an issue only for users who have used local authentication with LXCA and not remote authentication against external LDAP or ADFS servers. **CVE ID: CVE-2017-3745**	https://support.lenovo.com/us/en/product_security/LEN-13671	A-LEN-XCLAR-050717/125
Libav					
Libav					
DoS Overflow	28-06-2017	5	There is a heap-based buffer overflow in the function hpel_motion in mpegvideo_motion.c in libav 12.1. A crafted input can lead to a remote denial of service attack. **CVE ID: CVE-2017-9987**	https://bugzilla.libav.org/show_bug.cgi?id=1067	A-LIB-LIBAV-050717/126
Libdwarf Project					
Libdwarf					
DoS	28-06-2017	4.3	The _dwarf_decode_s_leb128_chk function in dwarf_leb.c in libdwarf through 28-06-2017 allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file. **CVE ID: CVE-2017-9998**	NA	A-LIB-LIBDW-050717/127
Libming					
Libming					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

DoS	28-06-2017	5	util/outputtxt.c in libming 0.4.8 mishandles memory allocation. A crafted input will lead to a remote denial of service (NULL pointer dereference) attack. **CVE ID: CVE-2017-9989**	https://github.com/libming/libming/issues/86	A-LIB-LIBMI-050717/128
Libming					
DoS	28-06-2017	5	The readEncUInt30 function in util/read.c in libming 0.4.8 mishandles memory allocation. A crafted input will lead to a remote denial of service (NULL pointer dereference) attack against parser.c. **CVE ID: CVE-2017-9988**	https://github.com/libming/libming/issues/85	A-LIB-LIBMI-050717/129
Libmtp Project					
Libmtp					
DoS Execute Code Overflow	23-06-2017	4.6	An integer overflow vulnerability in ptp-pack.c (ptp_unpack_OPL function) of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a mobile device into a personal computer through a USB cable. **CVE ID: CVE-2017-9832**	https://sourceforge.net/p/libmtp/mailman/message/35729062	A-LIB-LIBMT-050717/130
DoS Execute Code Overflow	23-06-2017	4.6	An integer overflow vulnerability in the ptp_unpack_EOS_CustomFuncEx function of the ptp-pack.c file of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a mobile device into a personal computer through a USB cable. **CVE ID: CVE-2017-9831**	https://sourceforge.net/p/libmtp/mailman/message/35735992/	A-LIB-LIBMT-050717/131
Libtiff					
Libtiff					
DoS Overflow	22-06-2017	4.3	In LibTIFF 4.0.7, the TIFFReadDirEntryLong8Array function in libtiff/tif_dirread.c mishandles a malloc operation, which allows attackers to cause a denial of	NA	A-LIB-LIBTI-050717/132

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			service (memory leak within the function _TIFFmalloc in tif_unix.c) via a crafted file. **CVE ID: CVE-2017-9815**		
DoS Overflow	26-06-2017	4.3	In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can lead to an abort resulting in a remote denial of service attack. **CVE ID: CVE-2017-9937**	NA	A-LIB-LIBTI-050717/133
DoS Overflow	26-06-2017	4.3	In LibTIFF 4.0.8, there is a memory leak in tif_jbig.c. A crafted TIFF document can lead to a memory leak resulting in a remote denial of service attack. **CVE ID: CVE-2017-9936**	NA	A-LIB-LIBTI-050717/134
DoS	29-06-2017	5	In LibTIFF 4.0.8, there is a assertion abort in the TIFFWriteDirectoryTagCheckedLong8Array function in tif_dirwrite.c. A crafted input will lead to a remote denial of service attack. **CVE ID: CVE-2017-10688**	http://bugzilla.maptools.org/show_bug.cgi?id=2712	A-LIB-LIBTI-050717/135
Execute Code Overflow Memory Corruption	26-06-2017	6.8	In LibTIFF 4.0.8, there is a heap-based buffer overflow in the t2p_write_pdf function in tools/tiff2pdf.c. This heap overflow could lead to different damages. For example, a crafted TIFF document can lead to an out-of-bounds read in TIFFCleanup, an invalid free in TIFFClose or t2p_free, memory corruption in t2p_readwrite_pdf_image, or a double free in t2p_free. Given these possibilities, it probably could cause arbitrary code execution. **CVE ID: CVE-2017-9935**	NA	A-LIB-LIBTI-050717/136
Libtorrent					
Libtorrent					
DoS Overflow	24-06-2017	4.3	The bdecode function in bdecode.cpp in libtorrent 1.1.3 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.	https://github.com/arvidn/libtorrent/issues/2099	A-LIB-LIBTO-050717/137

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-9847		
Lrzip Project					
Lrzip					
DoS Overflow	26-06-2017	4.3	In lrzip 0.631, a stack buffer overflow was found in the function get_fileinfo in lrzip.c:1074, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9929**	NA	A-LRZ-LRZIP-050717/ 138
DoS Overflow	26-06-2017	4.3	In lrzip 0.631, a stack buffer overflow was found in the function get_fileinfo in lrzip.c:979, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9928**	NA	A-LRZ-LRZIP-050717/ 139
Magicwinmail					
Winmail Server					
Execute Code Directory Traversal	24-06-2017	6.5	Winmail Server 6.1 allows remote code execution by authenticated users who leverage directory traversal in a netdisk.php move_folder_file call to move a .php file from the FTP folder into a web folder. **CVE ID: CVE-2017-9846**	NA	A-MAG-WINMA-050717/ 140
Matrixssl					
Matrixssl					
Overflow XSS	22-06-2017	6.4	An integer overflow vulnerability exists in the X509 certificate parsing functionality of InsideSecure MatrixSSL 3.8.7b. A specially crafted x509 certificate can cause a length counter to overflow, leading to a controlled out of bounds copy operation. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server application when initiating secure connection **CVE ID: CVE-2017-2782**	NA	A-MAT-MATRI-050717/ 141
Execute Code Overflow XSS	22-06-2017	7.5	An exploitable heap buffer overflow vulnerability exists in the X509 certificate parsing functionality of InsideSecure MatrixSSL 3.8.7b. A		A-MAT-MATRI-050717/ 142

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			specially crafted x509 certificate can cause a buffer overflow on the heap resulting in remote code execution. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server application when initiating secure connection. **CVE ID: CVE-2017-2781**		
Execute Code Overflow XSS	22-06-2017	7.5	An exploitable heap buffer overflow vulnerability exists in the X509 certificate parsing functionality of InsideSecure MatrixSSL 3.8.7b. A specially crafted x509 certificate can cause a buffer overflow on the heap resulting in remote code execution. To trigger this vulnerability, a specially crafted x509 certificate must be presented to the vulnerable client or server application when initiating secure connection. **CVE ID: CVE-2017-2780**		A-MAT-MATRI-050717/143
Meafinancial					
Algonquin State Bank Mobile Banking					
Gain Information	16-06-2017	4.3	The "Algonquin State Bank Mobile Banking" by Algonquin State Bank app 3.0.0 -- aka algonquin-state-bank-mobile-banking/id1089657735 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9581**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-ALGON-050717/144
Athen State Bank Mobile Banking					
Gain Information	16-06-2017	4.3	The athens-state-bank-mobile-banking/id719748589 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-	A-MEA-ATHEN-050717/145

			CVE ID: CVE-2017-9572	allow-login-credential-exposure-4d2f380b85c5	
Avb Bank Mobile Banking					
Gain Information	16-06-2017	4.3	The avb-bank-mobile-banking/id592565443 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9567**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-AVB B-050717/146
Blue Ridge Bank And Trust Co. Mobile Banking					
Gain Information	16-06-2017	4.3	The "Blue Ridge Bank and Trust Co. Mobile Banking" by Blue Ridge Bank and Trust Co. app 3.0.1 -- aka blue-ridge-bank-and-trust-co-mobile-banking/id699679197 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9597**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-BLUE -050717/147
Cbtx On The Go					
Gain Information	16-06-2017	4.3	The Citizens Bank (TX) cbtx-on-the-go/id892396102 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9569**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-CBTX -050717/148

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): **DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable**										

Ccb Mobile Banking					
Gain Information	16-06-2017	4.3	The Citizens Community Bank (TN) ccb-mobile-banking/id610030469 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9571**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-CCB M-050717/149
Cfb Mobile Banking					
Gain Information	16-06-2017	4.3	The "CFB Mobile Banking" by Citizens First Bank Wisconsin app 3.0.1 -- aka cfb-mobile-banking/id1081102805 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9596**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-CFB M-050717/150
Charlevoix State Bank					
Gain Information	16-06-2017	4.3	The "Charlevoix State Bank" by Charlevoix State Bank app 3.0.1 -- aka charlevoix-state-bank/id1128963717 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9583**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-CHARL-050717/151
Community Banks Cb2go					
Gain Information	16-06-2017	4.3	The community-banks-cb2go/id445828071 app 3.1.3 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-	https://medium.com/@chronic_9612/advisory-	A-MEA-COMMU-050717/152

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9564**	44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	
Community State Bank-lamar Mobile Banking					
Gain Information	16-06-2017	4.3	The "Community State Bank - Lamar Mobile Banking" by Community State Bank - Lamar app 3.0.3 -- aka community-state-bank-lamar-mobile-banking/id1083927885 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9585**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-COMMU-050717/153
Fccb					
Gain Information	16-06-2017	4.3	The First Citizens Community Bank fccb/id809930960 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9563**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FCCB-050717/154
First Citizens Bank-mobile Banking					
Gain Information	16-06-2017	4.3	The "First Citizens Bank-Mobile Banking" by First Citizens Bank (AL) app 3.0.0 -- aka first-citizens-bank-mobile-banking/id566037101 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-	A-MEA-FIRST-050717/155

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-9577	exposure-4d2f380b85c5	
First Security Bank Sleepy Eye Mobile					
Gain Information	16-06-2017	4.3	The first-security-bank-sleepy-eye-mobile/id870531890 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9565**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FIRST-050717/156
Fnb Kemp Mobile Banking					
Gain Information	16-06-2017	4.3	The "FNB Kemp Mobile Banking" by First National Bank of Kemp app 3.0.2 -- aka fnb-kemp-mobile-banking/id571448725 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9601**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FNB K-050717/157
Freedom 1st Credit Union Mobile Banking					
Gain Information	16-06-2017	4.3	The Freedom First freedom-1st-credit-union-mobile-banking/id1085229458 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9562**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FREED-050717/158
Fsb Dequeen Mobile Banking					
Gain	16-06-2017	4.3	The fsb-dequeen-mobile-	https://med	A-MEA-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Information			banking/id1091025340 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9566**	ium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	FSB D-050717/159
Fsby Mobile Banking					
Gain Information	16-06-2017	4.3	The "FSBY Mobile Banking" by First State Bank of Yoakum TX app 3.0.0 -- aka fsby-mobile-banking/id899136434 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9586**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FSBY -050717/160
Fvb Mobile Banking					
Gain Information	16-06-2017	4.3	The "FVB Mobile Banking" by First Volunteer Bank of Tennessee app 3.1.1 -- aka fvb-mobile-banking/id551018004 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9575**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-FVB M-050717/161
Hbo Mobile Banking					
Gain Information	16-06-2017	4.3	The "HBO Mobile Banking" by Heritage Bank of Ozarks app 3.0.0 -- aka hbo-mobile-banking/id860224933 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-	A-MEA-HBO M-050717/162

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9584**	for-ios-may-allow-login-credential-exposure-4d2f380b85c5	
Jmcu Mobile Banking					
Gain Information	16-06-2017	4.3	The "JMCU Mobile Banking" by Joplin Metro Credit Union app 3.0.0 -- aka jmcu-mobile-banking/id716065893 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9579**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-JMCU -050717/163
Kc Area Credit Union Mobile Banking					
Gain Information	16-06-2017	4.3	The "KC Area Credit Union Mobile Banking" by K C Area Credit Union app 3.0.1 -- aka kc-area-credit-union-mobile-banking/id1097607736 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9574**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-KC AR-050717/164
Middleton Community Bank Mobile Banking					
Gain Information	16-06-2017	4.3	The "Middleton Community Bank Mobile Banking" by Middleton Community Bank app 3.0.0 -- aka middleton-community-bank-mobile-banking/id721843238 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9576**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85	A-MEA-MIDDL-050717/165

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

				c5	
Morton Credit Union Mobile Banking					
Gain Information	16-06-2017	4.3	The "Morton Credit Union Mobile Banking" by Morton Credit Union app 3.0.1 -- aka morton-credit-union-mobile-banking/id1119623070 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9598**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-MORTO-050717/166
Mount Vernon Bank & Trust Mobile Banking					
Gain Information	16-06-2017	4.3	The mount-vernon-bank-trust-mobile-banking/id542706679 app 3.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9570**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-MOUNT-050717/167
Oculina Mobile Banking					
Gain Information	16-06-2017	4.3	The "Oculina Mobile Banking" by Oculina Bank app 3.0.0 -- aka oculina-mobile-banking/id867025690 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9593**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-OCULI-050717/168
Oritani Mobile Banking					
Gain Information	16-06-2017	4.3	The "Oritani Mobile Banking" by Oritani Bank app 3.0.0 -- aka oritani-mobile-banking/id778851066 for iOS	https://medium.com/@chronic_9612	A-MEA-ORITA-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9588**	/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	169
Pcsb Bank Mobile					
Gain Information	16-06-2017	4.3	The "PCSB BANK Mobile" by PCSB Bank app 3.0.4 -- aka pcsb-bank-mobile/id1067472090 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9587**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-PCSB -050717/170
Peoples Bank Tulsa					
Gain Information	16-06-2017	4.3	The "Peoples Bank Tulsa" by Peoples Bank - OK app 3.0.2 -- aka peoples-bank-tulsa/id1074279285 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9600**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-PEOPL-050717/171
Pioneer Bank & Trust Mobile Banking					
Gain Information	16-06-2017	4.3	The "Pioneer Bank & Trust Mobile Banking" by PIONEER BANK AND TRUST app 3.0.0 -- aka pioneer-bank-trust-mobile-banking/id603182861 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-	A-MEA-PIONE-050717/172

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			information via a crafted certificate. **CVE ID: CVE-2017-9580**	credential-exposure-4d2f380b85c5	
Rvcb Mobile					
Gain Information	16-06-2017	4.3	The "RVCB Mobile" by RVCB Mobile Banking app 3.0.0 -- aka rvcb-mobile/id757928895 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9578**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-RVCB -050717/173
Scsb Shelbyville Il Mobile Banking					
Gain Information	16-06-2017	4.3	The "SCSB Shelbyville IL Mobile Banking" by Shelby County State Bank app 3.0.0 -- aka scsb-shelbyville-il-mobile-banking/id938960224 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9589**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-SCSB -050717/174
Svb Mobile					
Gain Information	16-06-2017	4.3	The "SVB Mobile" by Sauk Valley Bank Mobile Banking app 3.0.0 -- aka svb-mobile/id796429885 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9594**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-SVB M-050717/175
Vision Bank					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Gain Information	16-06-2017	4.3	The MEA Financial vision-bank/id420406345 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9559**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-VISIO-050717/176
Your Legacy Federal Credit Union Mobile Banking					
Gain Information	16-06-2017	4.3	The "Your Legacy Federal Credit Union Mobile Banking" by Your Legacy Federal Credit Union app 3.0.1 -- aka your-legacy-federal-credit-union-mobile-banking/id919131389 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9592**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MEA-YOUR -050717/177
Microsoft					
Endpoint Protection; Forefront Endpoint Protection; Intune Endpoint Protection; Security Essentials; Windows Defender					
Execute Code Memory Corruption	29-06-2017	9.3	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on 32-bit versions of Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703 does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability". **CVE ID: CVE-2017-8558**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8558	A-MIC-ENDPO-050717/178
Internet Explorer					
Execute	27-06-2017	7.6	Internet Explorer 6, Internet Explorer	NA	A-MIC-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Code Overflow			7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 allows remote attackers to execute arbitrary code. **CVE ID: CVE-2014-6354**		INTER-050717/179
Mosquitto Project					
Mosquitto					
Gain Information	25-06-2017	2.1	In Mosquitto through 1.4.12, mosquitto.db (aka the persistence file) is world readable, which allows local users to obtain sensitive MQTT topic information. **CVE ID: CVE-2017-9868**	https://github.com/eclipse/mosquitto/issues/468	A-MOS-MOSQU-050717/180
Myfpcu					
Financial Plus Mobile Banking					
Gain Information	16-06-2017	4.3	The financial-plus-mobile-banking/id731070564 app 3.0.3 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9568**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MYF-FINAN-050717/181
Mypcb					
Phelps County Bank					
Gain Information	16-06-2017	4.3	The "PCB Mobile" by Phelps County Bank app 3.0.2 -- aka pcb-mobile/id436891295 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9591**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-MYP-PHELP-050717/182
Northadamsbank					
Nasb Mobile Bank					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Gain Information	16-06-2017	4.3	The North Adams State Bank (Ursa) nasb-mobile-banking/id980573797 app 3.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9573**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-NOR-NASB -050717/183
Ntop					
Ntopng					
XSS	26-06-2017	4.3	ntopng before 3.0 allows XSS because GET and POST parameters are improperly validated. **CVE ID: CVE-2017-7416**	https://github.com/ntop/ntopng/blob/3.0/CHANGELOG.md	A-NTO-NTOPN-050717/184
HTTP Response Splitting	26-06-2017	5	ntopng before 3.0 allows HTTP Response Splitting. **CVE ID: CVE-2017-7459**	https://github.com/ntop/ntopng/blob/3.0/CHANGELOG.md	A-NTO-NTOPN-050717/185
DoS	26-06-2017	5	The NetworkInterface::getHost function in NetworkInterface.cpp in ntopng before 3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty field that should have contained a hostname or IP address. **CVE ID: CVE-2017-7458**	NA	A-NTO-NTOPN-050717/186
Nuevomailer					
Nuevomailer					
Execute Code Sql	19-06-2017	7.5	SQL injection vulnerability in rdr.php in nuevoMailer version 6.0 and earlier allows remote attackers to execute arbitrary SQL commands via the "r" parameter. **CVE ID: CVE-2017-9730**	https://www.exploit-db.com/exploits/42193/	A-NUE-NUEVO-050717/187
Opendaylight					
Defense4all					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	27-06-2017	6.5	OpenDaylight defense4all 1.1.0 and earlier allows remote authenticated users to write report data to arbitrary files. **CVE ID: CVE-2014-8149**	https://wiki.opendaylight.org/view/Security_Advisories	A-OPE-DEFEN-050717/188
Openvpn					
Openvpn					
NA	27-06-2017	4	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service by authenticated remote attacker via sending a certificate with an embedded NULL character. **CVE ID: CVE-2017-7522**	https://community.openvpn.net/openvpn/wiki/VulnerabilitiesFixedInOpenVPN243	A-OPE-OPENV-050717/189
NA	27-06-2017	5	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service when receiving malformed IPv6 packet. **CVE ID: CVE-2017-7508**	https://community.openvpn.net/openvpn/wiki/VulnerabilitiesFixedInOpenVPN243	A-OPE-OPENV-050717/190
Openwebif Project					
Openwebif					
Execute Code	21-06-2017	10	An issue was discovered in the OpenWebif plugin through 1.2.4 for E2 open devices. The saveConfig function of "plugin/controllers/models/config.py" performs an eval() call on the contents of the "key" HTTP GET parameter. This allows an unauthenticated remote attacker to execute arbitrary Python code or OS commands via api/saveconfig. **CVE ID: CVE-2017-9807**	https://github.com/E2OpenPlugins/e2openplugin-OpenWebif/issues/620	A-OPE-OPENW-050717/191
Piwigo					
Piwigo					
XSS	24-06-2017	3.5	Cross-site scripting (XSS) vulnerability in Piwigo 2.9.1 allows remote authenticated administrators to inject arbitrary web script or HTML via the virtual_name parameter to /admin.php (i.e., creating a virtual album).	https://github.com/Piwigo/Piwigo/issues/716	A-PIW-PIWIG-050717/192

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-9836		
Gain Information	29-06-2017	5	Piwigo through 2.9.1 allows remote attackers to obtain sensitive information about the descriptive name of a permalink by examining the redirect URL that is returned in a request for the permalink ID number of a private album. The permalink ID numbers are easily guessed. **CVE ID: CVE-2017-10679**	https://github.com/Piwigo/Piwigo/issues/723	A-PIW-PIWIG-050717/193
CSRF	29-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Piwigo through 2.9.1 allows remote attackers to hijack the authentication of users for requests to unlock albums via a crafted request. **CVE ID: CVE-2017-10681**	https://github.com/Piwigo/Piwigo/issues/721	A-PIW-PIWIG-050717/194
CSRF	29-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Piwigo through 2.9.1 allows remote attackers to hijack the authentication of users for requests to change a private album to public via a crafted request. **CVE ID: CVE-2017-10680**	https://github.com/Piwigo/Piwigo/issues/721	A-PIW-PIWIG-050717/195
CSRF	29-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Piwigo through 2.9.1 allows remote attackers to hijack the authentication of users for requests to delete permalinks via a crafted request. **CVE ID: CVE-2017-10678**	https://github.com/Piwigo/Piwigo/issues/721	A-PIW-PIWIG-050717/196
NA	24-06-2017	7.5	The ws_session_logout function in Piwigo 2.9.1 and earlier does not properly delete user login cookies, which allows remote attackers to gain access via cookie reuse. **CVE ID: CVE-2017-9837**	https://github.com/Piwigo/Piwigo/issues/717	A-PIW-PIWIG-050717/197
Execute Code Sql	29-06-2017	7.5	SQL injection vulnerability in the administrative backend in Piwigo through 2.9.1 allows remote users to execute arbitrary SQL commands via the cat_false or cat_true parameter in the comments or status page to cat_options.php. **CVE ID: CVE-2017-10682**	https://github.com/Piwigo/Piwigo/issues/724	A-PIW-PIWIG-050717/198

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Projectsend					
Projectsend					
Execute Code	18-06-2017	7.5	install/make-config.php in ProjectSend r754 allows remote attackers to execute arbitrary PHP code via the dbprefix parameter, related to replacing TABLES_PREFIX in the configuration file. **CVE ID: CVE-2017-9741**	https://github.com/XiaoZhis/ProjectSend/issues/1	A-PRO-PROJE-050717/199
Qemu					
Qemu					
DoS	16-06-2017	1.9	QEMU (aka Quick Emulator), when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving megasas command processing. **CVE ID: CVE-2017-9503**	https://bugzilla.redhat.com/show_bug.cgi?id=1459477	A-QEM-QEMU-050717/200
DoS	16-06-2017	1.9	QEMU (aka Quick Emulator), when built with USB xHCI controller emulator support, allows local guest OS privileged users to cause a denial of service (infinite recursive call) via vectors involving control transfer descriptors sequencing. **CVE ID: CVE-2017-9375**	http://git.qemu.org/?p=qemu.git;a=commit;h=96d87bdda3919bb16f754b3d3fd1227e1f38f13c	A-QEM-QEMU-050717/201
DoS Overflow	16-06-2017	1.9	Memory leak in QEMU (aka Quick Emulator), when built with IDE AHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the AHCI device. **CVE ID: CVE-2017-9373**	http://git.qemu.org/?p=qemu.git;a=commit;h=d68f0f778e7f4fbd674627274267f269e40f0b04	A-QEM-QEMU-050717/202
DoS Overflow	16-06-2017	2.1	Memory leak in QEMU (aka Quick Emulator), when built with USB EHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the device. **CVE ID: CVE-2017-9374**	https://bugzilla.redhat.com/show_bug.cgi?id=1459132	A-QEM-QEMU-050717/203
Radare					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Radare2					
DoS	19-06-2017	4.3	The cmd_info function in libr/core/cmd_info.c in radare2 1.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted binary file. **CVE ID: CVE-2017-9762**	https://github.com/radare/radare2/issues/7726	A-RAD-RADAR-050717/204
DoS Overflow	19-06-2017	4.3	The find_eoq function in libr/core/cmd.c in radare2 1.5.0 allows remote attackers to cause a denial of service (heap-based out-of-bounds read and application crash) via a crafted binary file. **CVE ID: CVE-2017-9761**	https://github.com/radare/radare2/commit/00e8f205475332d7842d0f0d1481eeab4e83017c	A-RAD-RADAR-050717/205
Redhat					
Automatic Bug Reporting Tool					
Gain Information	26-06-2017	1.9	The kernel-invoked coredump processor in Automatic Bug Reporting Tool (ABRT) does not properly check the ownership of files before writing core dumps to them, which allows local users to obtain sensitive information by leveraging write permissions to the working directory of a crashed application. **CVE ID: CVE-2015-3142**	https://bugzilla.redhat.com/show_bug.cgi?id=1212818	A-RED-AUTOM-050717/206
Gain Information	26-06-2017	2.1	The event scripts in Automatic Bug Reporting Tool (ABRT) uses world-readable permission on a copy of sosreport file in problem directories, which allows local users to obtain sensitive information from /var/log/messages via unspecified vectors. **CVE ID: CVE-2015-1870**	https://bugzilla.redhat.com/show_bug.cgi?id=1212868	A-RED-AUTOM-050717/207
Gluster Storage					
Execute Code Gain Privileges	27-06-2017	7.2	Red Hat Gluster Storage RPM Package 3.2 allows local users to gain privileges and execute arbitrary code as root. **CVE ID: CVE-2015-1795**	https://bugzilla.redhat.com/show_bug.cgi?id=1200927	A-RED-GLUST-050717/208
Satellite					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Gain Information	27-06-2017	3.5	Satellite 6.1.0 allows remote authenticated users to read administrator bookmarks. **CVE ID: CVE-2015-7582**	https://bugzilla.redhat.com/show_bug.cgi?id=1192414	A-RED-SATEL-050717/209
Virtio-win					
DoS	26-06-2017	5	The NetKVM Windows Virtio driver allows remote attackers to cause a denial of service (guest crash) via a crafted length value in an IP packet, as demonstrated by a value that does not account for the size of the IP options. **CVE ID: CVE-2015-3215**	https://github.com/YanVugenfirer/kvm-guest-drivers-windows/commit/fbfa4d1083ea84c5429992ca3e996d7d4fbc8238	A-RED-VIRTI-050717/210
Samsung					
Magician					
NA	21-06-2017	8.3	Samsung Magician 5.0 fails to validate TLS certificates for HTTPS software update traffic. Prior to version 5.0, Samsung Magician uses HTTP for software updates. **CVE ID: CVE-2017-3218**	NA	A-SAM-MAGIC-050717/211
SBW					
State Bank Of Waterloo Mobile Banking					
Gain Information	16-06-2017	4.3	The "State Bank of Waterloo Mobile Banking" by State Bank of Waterloo app 3.0.2 -- aka state-bank-of-waterloo-mobile-banking/id555321714 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9590**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-SBW-STATE-050717/212
Sitecore					
Sitecore.net					
XSS	23-06-2017	4.3	Sitecore.NET 7.1 through 7.2 has a Cross Site Scripting Vulnerability via	NA	A-SIT-SITEC-

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			the searchStr parameter to the /Search-Results URI. **CVE ID: CVE-2017-9356**		050717/ 213
Spip					
Spip					
Execute Code	17-06-2017	7.5	SPIP 3.1.x before 3.1.6 and 3.2.x before Beta 3 does not remove shell metacharacters from the host field, allowing a remote attacker to cause remote code execution. **CVE ID: CVE-2017-9736**	https://core.spip.net/projects/spip/repository/revisions/23594	A-SPI-SPIP-050717/ 214
Stalin Project					
Stalin					
	27-06-2017	2.1	stalin 0.11-5 allows local users to write to arbitrary files. **CVE ID: CVE-2015-8697**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=808730	A-STA-STALI-050717/ 215
Sthttpd Project					
Sthttpd					
DoS Overflow	29-06-2017	6.8	Heap-based Buffer Overflow in the de_dotdot function in libhttpd.c in sthttpd before 2.27.1 allows remote attackers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a crafted filename. **CVE ID: CVE-2017-10671**	NA	A-STH-STHTT-050717/ 216
Symantec					
Messaging Gateway					
Execute Code	26-06-2017	10	The Symantec Messaging Gateway can encounter an issue of remote code execution, which describes a situation whereby an individual may obtain the ability to execute commands remotely on a target machine or in a target process. **CVE ID: CVE-2017-6326**	https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=2017062	A-SYM-MESSA-050717/ 217

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

				1_00	
Teamspeak					
Teamspeak Client					
DoS	27-06-2017	5	TeamSpeak Client 3.0.19 allows remote attackers to cause a denial of service (application crash) via the &#5610; Unicode character followed by the &#3903; Unicode character. **CVE ID: CVE-2017-9982**	NA	A-TEA-TEAMS-050717/218
Trihedral					
Vtscada					
Execute Code XSS	21-06-2017	4.3	A Cross-Site Scripting issue was discovered in Trihedral VTScada Versions prior to 11.2.26. A cross-site scripting vulnerability may allow JavaScript code supplied by the attacker to execute within the user's browser. **CVE ID: CVE-2017-6053**	NA	A-TRI-VTSCA-050717/219
Gain Information	21-06-2017	5	An Information Exposure issue was discovered in Trihedral VTScada Versions prior to 11.2.26. Some files are exposed within the web server application to unauthenticated users. These files may contain sensitive configuration information. **CVE ID: CVE-2017-6045**	NA	A-TRI-VTSCA-050717/220
NA	21-06-2017	7.8	A Resource Consumption issue was discovered in Trihedral VTScada Versions prior to 11.2.26. The client does not properly validate the input or limit the amount of resources that are utilized by an attacker, which can be used to consume more resources than are available. **CVE ID: CVE-2017-6043**	NA	A-TRI-VTSCA-050717/221
Uclibc					
Uclibc					
NA	16-06-2017	5	In uClibc 0.9.33.2, there is stack exhaustion (uncontrolled recursion) in the check_dst_limits_calc_pos_1 function in misc/regex/regexec.c when processing a crafted regular	http://openwall.com/lists/oss-security/2017/06/16/4	A-UCL-UCLIB-050717/222

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			expression. **CVE ID: CVE-2017-9729**		
NA	16-06-2017	7.5	In uClibc 0.9.33.2, there is an out-of-bounds read in the get_subexp function in misc/regex/regexec.c when processing a crafted regular expression. **CVE ID: CVE-2017-9728**	http://openwall.com/lists/oss-security/2017/06/16/4	A-UCL-UCLIB-050717/223
Wawacu					
Wawa Employees Credit Union Mobile					
Gain Information	16-06-2017	4.3	The wawa-employees-credit-union-mobile/id1158082793 app 4.0.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-9558**	https://medium.com/@chronic_9612/advisory-44-credit-union-apps-for-ios-may-allow-login-credential-exposure-4d2f380b85c5	A-WAW-WAWA -050717/224
Websitebaker					
Websitebaker					
Execute Code	21-06-2017	7.5	install\save.php in WebsiteBaker v2.10.0 allows remote attackers to execute arbitrary PHP code via the database_username parameter. **CVE ID: CVE-2017-9771**	https://github.com/XiaoZhis/ProjectSend/issues/3	A-WEB-WEBSI-050717/225
Wireshark					
Wireshark					
DoS	21-06-2017	5	In Wireshark 2.2.7, PROFINET IO data with a high recursion depth allows remote attackers to cause a denial of service (stack exhaustion) in the dissect_IODWriteReq function in plugins/profinet/packet-dcerpc-pn-io.c. **CVE ID: CVE-2017-9766**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=d6e888400ba64de3147d1111a4c23edf389b0000	A-WIR-WIRES-050717/226
Zenbership					
Zenbership					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Sql	19-06-2017	6.5	SQL Injection exists in admin/index.php in Zenbership 1.0.8 via the filters array parameter, exploitable by a privileged account. **CVE ID: CVE-2017-9759**	NA	A-ZEN-ZENBE-050717/227
Zen-cart					
Zen Cart					
XSS	28-06-2017	4.3	In index.php in Zen Cart 1.6.0, the products_id parameter can cause XSS. **CVE ID: CVE-2017-10667**	NA	A-ZEN-ZEN C-050717/228
Zohocorp					
Manageengine Firewall Analyzer					
Directory Traversal	27-06-2017	4	Directory traversal vulnerability in ManageEngine Firewall Analyzer before 8.0. **CVE ID: CVE-2015-7780**	NA	A-ZOH-MANAG-050717/229
NA	27-06-2017	5	ManageEngine Firewall Analyzer before 8.0 does not restrict access permissions. **CVE ID: CVE-2015-7781**	NA	A-ZOH-MANAG-050717/230
Application; OS (A/OS)					
Exiv2/Redhat					
Exiv2/Enterprise Linux					
DoS	26-06-2017	5	There is an invalid free in Image::printIFDStructure that leads to a Segmentation fault in Exiv2 0.26. A crafted input will lead to a remote denial of service attack. **CVE ID: CVE-2017-9953**	https://bugzilla.redhat.com/show_bug.cgi?id=1465061	A-OS-EXI-EXIV2-050717/231
Libtiff/Opensuse Project					
Libtiff/Opensuse					
DoS	26-06-2017	4.3	LibTIFF 4.0.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted TIFF image to the (1) checkInkNamesString function in tif_dir.c in the thumbnail tool, (2) compresscontig function in tiff2bw.c in the tiff2bw tool, (3) putcontig8bitCIELab function in tif_getimage.c in the tiff2rgba tool, LZWPreDecode function in tif_lzw.c in	http://bugzilla.maptools.org/show_bug.cgi?id=2484	A-OS-LIB-LIBTI-050717/232

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			the (4) tiff2ps or (5) tiffdither tool, (6) NeXTDecode function in tif_next.c in the tiffmedian tool, or (7) TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool. **CVE ID: CVE-2014-8127**		
Operating System (OS)					
Belden Hirschmann					
Gecko Lite Managed Switch Firmware					
NA	29-06-2017	4.3	A Server-Side Request Forgery issue was discovered in Belden Hirschmann GECKO Lite Managed switch, Version 2.0.00 and prior versions. The web server receives a request, but does not sufficiently verify that the request is being sent to the expected destination. **CVE ID: CVE-2017-6036**	https://ics-cert.us-cert.gov/advisories/ICSA-17-026-02A	O-BEL-GECKO-050717/233
Gecko Lite Managed Switch Firmware					
Gain Information	29-06-2017	5	An Information Exposure issue was discovered in Belden Hirschmann GECKO Lite Managed switch, Version 2.0.00 and prior versions. Non-sensitive information can be obtained anonymously. **CVE ID: CVE-2017-6040**	https://ics-cert.us-cert.gov/advisories/ICSA-17-026-02A	O-BEL-GECKO-050717/234
CSRF	29-06-2017	5.8	A Cross-Site Request Forgery issue was discovered in Belden Hirschmann GECKO Lite Managed switch, Version 2.0.00 and prior versions. The web application does not sufficiently verify that requests were provided by the user who submitted the request. **CVE ID: CVE-2017-6038**	https://ics-cert.us-cert.gov/advisories/ICSA-17-026-02A	O-BEL-GECKO-050717/235
Cambium Networks					
Epmp 1000 Firmware; Epmp 1000 Hotspot Firmware; Epmp 2000 Firmware; Epmp Elevate Firmware					
NA	21-06-2017	6	An Improper Access Control issue was discovered in Cambium Networks ePMP. After a valid user has used SNMP configuration export, an attacker is able to remotely	NA	O-CAM-EPMP -050717/236

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			trigger device configuration backups using specific MIBs. These backups lack proper access control and may allow access to sensitive information and possibly allow for configuration changes. **CVE ID: CVE-2017-7918**		
Gain Privileges	21-06-2017	6.5	An Improper Privilege Management issue was discovered in Cambium Networks ePMP. The privileges for SNMP community strings are not properly restricted, which may allow an attacker to gain access to sensitive information and possibly allow for configuration changes. **CVE ID: CVE-2017-7922**	NA	O-CAM-EPMP -050717/237
EMC					
Isilon Onefs					
NA	21-06-2017	9	EMC Isilon OneFS 8.0.1.0, 8.0.0 - 8.0.0.3, 7.2.0 - 7.2.1.4, 7.1.x is affected by a privilege escalation vulnerability that could potentially be exploited by attackers to compromise the affected system. **CVE ID: CVE-2017-4988**	http://www.securityfocus.com/archive/1/540755/30/0/threaded	O-EMC-ISILO-050717/238
Vnx1 Firmware;Vnx2 Firmware					
Execute Code	19-06-2017	4.4	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, a local authenticated user can load a maliciously crafted file in the search path which may potentially allow the attacker to execute arbitrary code on the targeted VNX Control Station system, aka an uncontrolled search path vulnerability. **CVE ID: CVE-2017-4987**	http://www.securityfocus.com/archive/1/540738/30/0/threaded	O-EMC-VNX1 -050717/239
NA	19-06-2017	7.2	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, a local authenticated user may potentially escalate their privileges to root due to authorization checks not being performed on certain perl scripts.	http://www.securityfocus.com/archive/1/540738/30/0/threaded	O-EMC-VNX1 -050717/240

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			This may potentially be exploited by an attacker to run arbitrary commands as root on the targeted VNX Control Station system. **CVE ID: CVE-2017-4985**		
Execute Code	19-06-2017	10	In EMC VNX2 versions prior to OE for File 8.1.9.211 and VNX1 versions prior to OE for File 7.1.80.8, an unauthenticated remote attacker may be able to elevate their permissions to root through a command injection. This may potentially be exploited by an attacker to run arbitrary code with root-level privileges on the targeted VNX Control Station system, aka remote code execution. **CVE ID: CVE-2017-4984**	http://www.securityfocus.com/archive/1/540738/30/0/threaded	O-EMC-VNX1 -050717/241
Foscam					
C1 Indoor Hd Camera Firmware					
Directory Traversal	21-06-2017	4	An exploitable directory traversal vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause the application to read a file from disk but a failure to adequately filter characters results in allowing an attacker to specify a file outside of a directory. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2829**	NA	O-FOS-C1 IN-050717/242
Overflow	21-06-2017	5	An exploitable buffer overflow vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause a buffer overflow resulting in overwriting arbitrary data. An attacker can simply send an		O-FOS-C1 IN-050717/243

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2831**		
Overflow	21-06-2017	5	An exploitable buffer overflow vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can cause a buffer overflow resulting in overwriting arbitrary data. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2830**		O-FOS-C1 IN-050717/244
NA	21-06-2017	6.5	An exploitable command injection vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can allow for a user to inject arbitrary shell characters during account creation resulting in command injection. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2828**	NA	O-FOS-C1 IN-050717/245
NA	21-06-2017	6.5	An exploitable command injection vulnerability exists in the web management interface used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.37. A specially crafted HTTP request can allow for a user to inject arbitrary shell characters during account creation resulting in command injection. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2827**	NA	O-FOS-C1 IN-050717/246
Execute Code	27-06-2017	7.5	In the web management interface in Foscam C1 Indoor HD Camera running application firmware	NA	O-FOS-C1 IN-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			2.52.2.37, a specially crafted HTTP request can allow for a user to inject arbitrary data in the "msmtprc" configuration file resulting in command execution. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2843**		247
Execute Code	27-06-2017	7.5	In the web management interface in Foscam C1 Indoor HD Camera running application firmware 2.52.2.37, a specially crafted HTTP request can allow for a user to inject arbitrary data in the "msmtprc" configuration file resulting in command execution. An attacker can simply send an HTTP request to the device to trigger this vulnerability. **CVE ID: CVE-2017-2842**	NA	O-FOS-C1 IN-050717/248
Huawei					
P7-l09 Firmware					
DoS	27-06-2017	5	Huawei Ascend P7 allows remote attackers to cause a denial of service (phone process crash). **CVE ID: CVE-2015-2245**	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-414153.htm	O-HUA-P7-L0-050717/249
Linux					
Linux Kernel					
Gain Information	17-06-2017	2.1	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time. **CVE ID: CVE-2017-1000380**	NA	O-LIN-LINUX-050717/250
NA	19-06-2017	7.2	The Linux Kernel running on AMD64 systems will sometimes map the contents of PIE executable, the heap	https://access.redhat.com/security/cve/C	O-LIN-LINUX-050717/

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			or ld.so to where the stack is mapped allowing attackers to more easily manipulate the stack. Linux Kernel version 4.11.5 is affected. **CVE ID: CVE-2017-1000379**	VE-2017-1000379	251
NA	19-06-2017	7.2	The offset2lib patch as used by the Linux Kernel contains a vulnerability, if RLIMIT_STACK is set to RLIM_INFINITY and 1 Gigabyte of memory is allocated (the maximum under the 1/4 restriction) then the stack will be grown down to 0x80000000, and as the PIE binary is mapped above 0x80000000 the minimum distance between the end of the PIE binary's read-write segment and the start of the stack becomes small enough that the stack guard page can be jumped over by an attacker. This affects Linux Kernel version 4.11.5. This is a different issue than CVE-2017-1000370 and CVE-2017-1000365. This issue appears to be limited to i386 based systems. **CVE ID: CVE-2017-1000371**	https://access.redhat.com/security/cve/CVE-2017-1000371	O-LIN-LINUX-050717/252
NA	19-06-2017	7.2	The offset2lib patch as used in the Linux Kernel contains a vulnerability that allows a PIE binary to be execve()'ed with 1GB of arguments or environmental strings then the stack occupies the address 0x80000000 and the PIE binary is mapped above 0x40000000 nullifying the protection of the offset2lib patch. This affects Linux Kernel version 4.11.5 and earlier. This is a different issue than CVE-2017-1000371. This issue appears to be limited to i386 based systems. **CVE ID: CVE-2017-1000370**	https://access.redhat.com/security/cve/CVE-2017-1000370	O-LIN-LINUX-050717/253
Bypass	19-06-2017	7.2	The Linux Kernel imposes a size restriction on the arguments and environmental strings passed	https://access.redhat.com/security/cve/C	O-LIN-LINUX-050717/

			through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23. **CVE ID: CVE-2017-1000365**	VE-2017-1000365	254
DoS	28-06-2017	7.2	The intr function in sound/oss/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a "double fetch" vulnerability. **CVE ID: CVE-2017-9986**	NA	O-LIN-LINUX-050717/255
DoS	28-06-2017	7.2	The snd_msndmidi_input_read function in sound/isa/msnd/msnd_midi.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a "double fetch" vulnerability. **CVE ID: CVE-2017-9985**	NA	O-LIN-LINUX-050717/256
DoS	28-06-2017	7.2	The snd_msnd_interrupt function in sound/isa/msnd/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer	NA	O-LIN-LINUX-050717/257

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			between two kernel reads of that value, aka a "double fetch" vulnerability. **CVE ID: CVE-2017-9984**		
Overflow Bypass	19-06-2017	10	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010). **CVE ID: CVE-2017-1000364**	https://www.suse.com/support/kb/doc/?id=7020973	O-LIN-LINUX-050717/258
Microsoft					
Windows 10; Windows 7; Windows 8.1; Windows Rt 8.1; Windows Server 2008; Windows Server 2012; Windows Server 2016					
Gain Information	29-06-2017	1.9	The kernel in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an authenticated attacker to obtain memory contents via a specially crafted application. **CVE ID: CVE-2017-8554**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8554	O-MIC-WINDO-050717/259
Windows 10; Windows Server 2016					
Gain Information	29-06-2017	2.1	The kernel in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to obtain information via a specially crafted application, aka "Microsoft Graphics Component Information Disclosure Vulnerability." **CVE ID: CVE-2017-8575**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8575	O-MIC-WINDO-050717/260
NA	29-06-2017	6.9	The DirectX component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka "DirectX Elevation of Privilege	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8579	O-MIC-WINDO-050717/261

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Vulnerability." **CVE ID: CVE-2017-8579**		
NA	29-06-2017	6.9	The graphics component in Microsoft Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an authenticated attacker to run arbitrary code in kernel mode via a specially crafted application, aka "Microsoft Graphics Component Elevation of Privilege Vulnerability." **CVE ID: CVE-2017-8576**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8576	O-MIC-WINDO-050717/262
Netbsd					
Netbsd					
Execute Code	19-06-2017	7.5	The NetBSD qsort() function is recursive, and not randomized, an attacker can construct a pathological input array of N elements that causes qsort() to deterministically recurse N/4 times. This allows attackers to consume arbitrary amounts of stack memory and manipulate stack memory to assist in arbitrary code execution attacks. This affects NetBSD 7.1 and possibly earlier versions. **CVE ID: CVE-2017-1000378**	NA	O-NET-NETBS-050717/263
Execute Code Overflow	19-06-2017	7.5	NetBSD maps the run-time link-editor ld.so directly below the stack region, even if ASLR is enabled, this allows attackers to more easily manipulate memory leading to arbitrary code execution. This affects NetBSD 7.1 and possibly earlier versions. **CVE ID: CVE-2017-1000375**	NA	O-NET-NETBS-050717/264
Execute Code Bypass	19-06-2017	7.5	A flaw exists in NetBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using certain setuid binaries. This affects NetBSD 7.1 and possibly earlier versions. **CVE ID: CVE-2017-1000374**	NA	O-NET-NETBS-050717/265
Openbsd					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Openbsd					
Execute Code Bypass	19-06-2017	7.5	A flaw exists in OpenBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using setuid binaries such as /usr/bin/at. This affects OpenBSD 6.1 and possibly earlier versions. **CVE ID: CVE-2017-1000372**	NA	O-OPE-OPENB-050717/266
Oracle					
Solaris					
DoS	22-06-2017	4.6	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE ID: CVE-2017-3630**	http://www.oracle.com/technetwork/security-advisory/alert-CVE-2017-3629-3757403.html	O-ORA-SOLAR-050717/267
NA	22-06-2017	7.2	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris.	http://www.oracle.com/technetwork/security-advisory/alert-CVE-2017-3629-3757403.html	O-ORA-SOLAR-050717/268

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID: CVE-2017-3629**		
Samsung					
Samsung Mobile					
DoS	27-06-2017	2.1	Samsung Gallery in the Samsung Galaxy S6 allows local users to cause a denial of service (process crash). **CVE ID: CVE-2015-7898**	https://bugs.chromium.org/p/project-zero/issues/detail?id=500&redir=1	O-SAM-SAMSU-050717/269
DoS	27-06-2017	2.1	Samsung Gallery on the Samsung Galaxy S6 allows local users to cause a denial of service (process crash). **CVE ID: CVE-2015-7895**	https://bugs.chromium.org/p/project-zero/issues/detail?id=497&redir=1	O-SAM-SAMSU-050717/270
Operating System; Application (OS/A)					
Canonical/GNU					
Ubuntu Linux/Glibc					
DoS	27-06-2017	5	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash). **CVE ID: CVE-2015-5180**	https://sourceware.org/bugzilla/attachment.cgi?id=8492	O-A-CAN-UBUNT-050717/271
Fedoraproject/Midas					
Fedora/Elog					
NA	27-06-2017	5	elog 3.1.1 allows remote attackers to post data as any username in the logbook. **CVE ID: CVE-2016-6342**	https://bugzilla.redhat.com/show_bug.cgi?id=1371328	O-A-FED-FEDOR-050717/272

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable